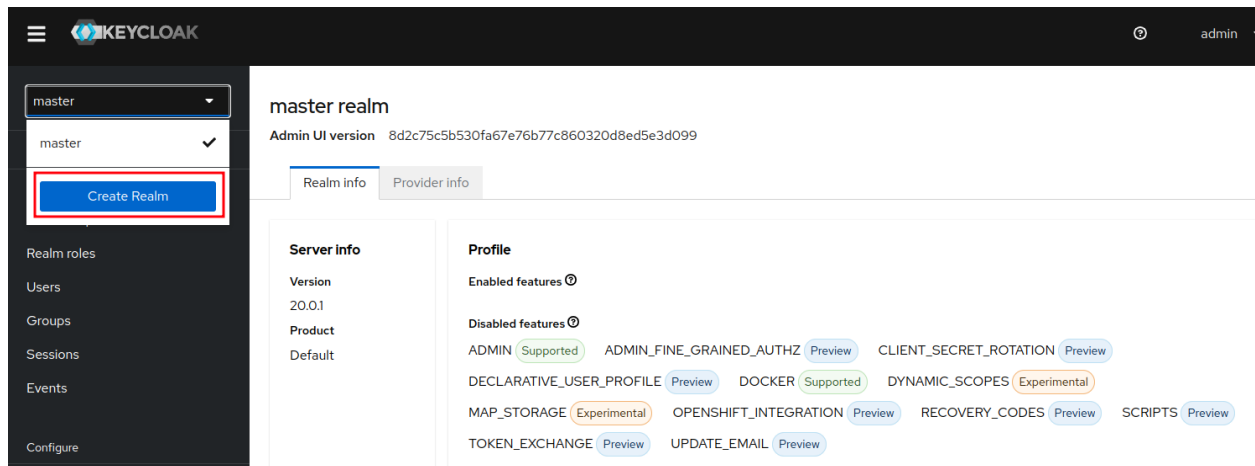
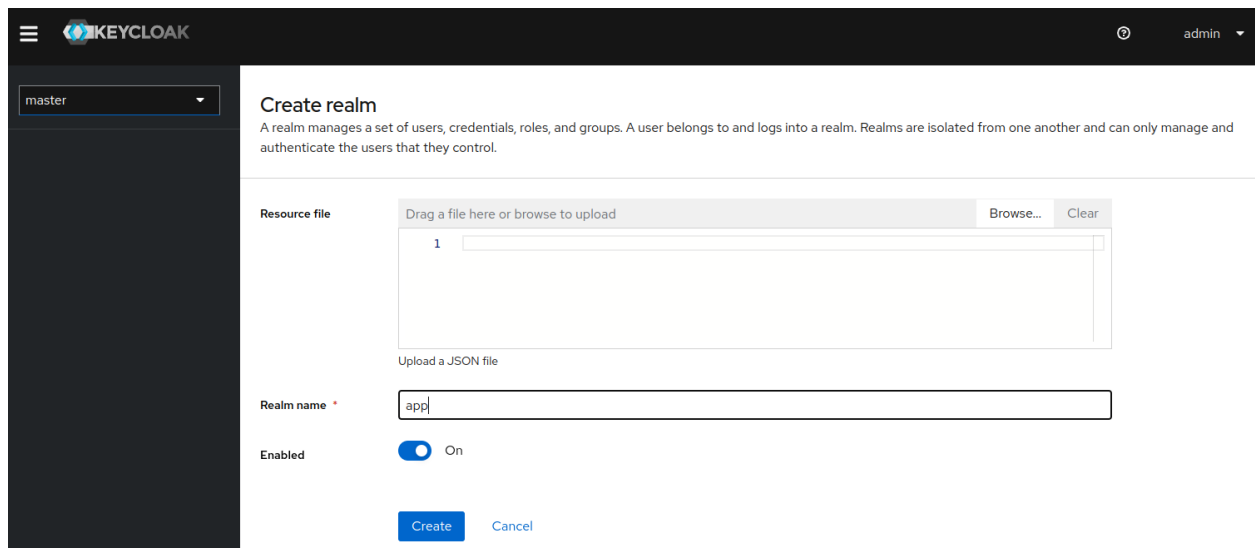


Create a new realm, client and users (Keycloak version 20)

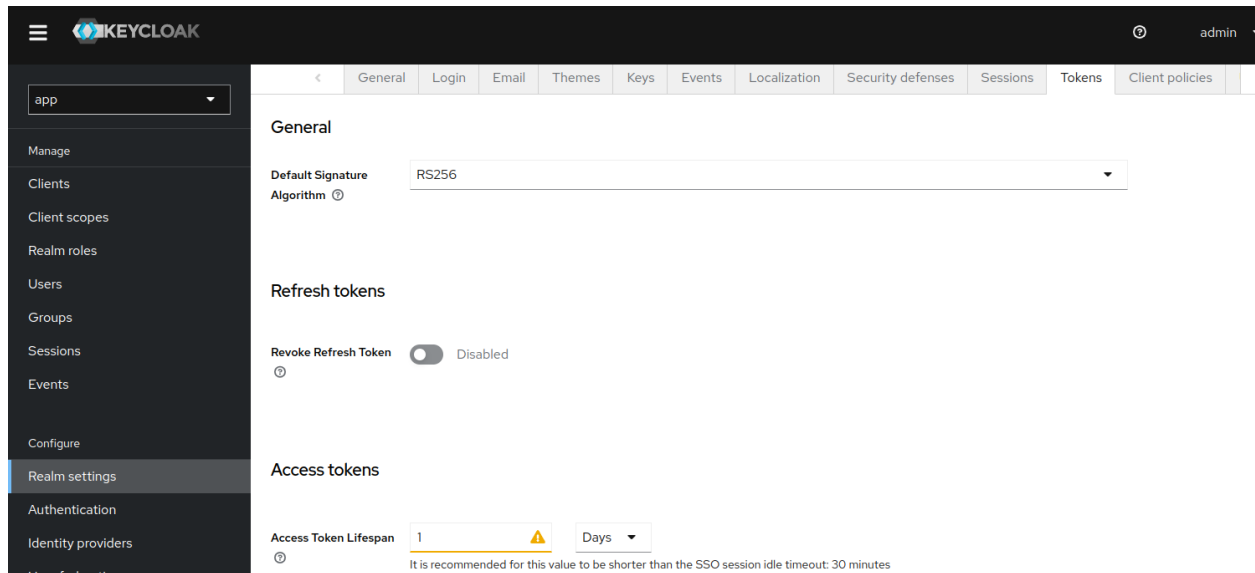
1) Enter inside the Keycloak admin console (<http://localhost:8080/admin>). The default username and password is **admin**. Move the mouse over **Master** and click in the Create realm button.



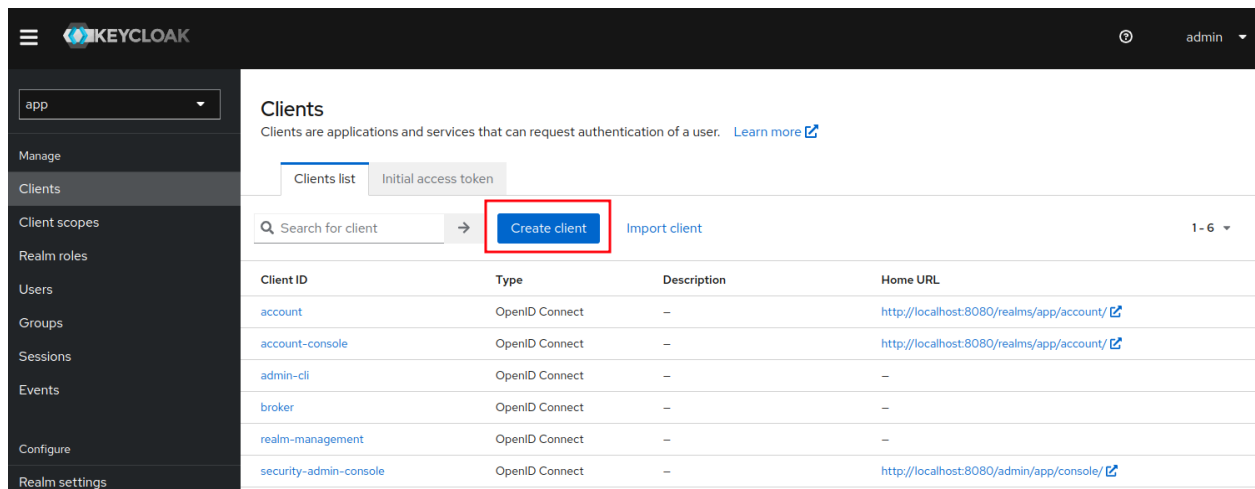
2) Fill the name of the realm with **app** and click the Create button.



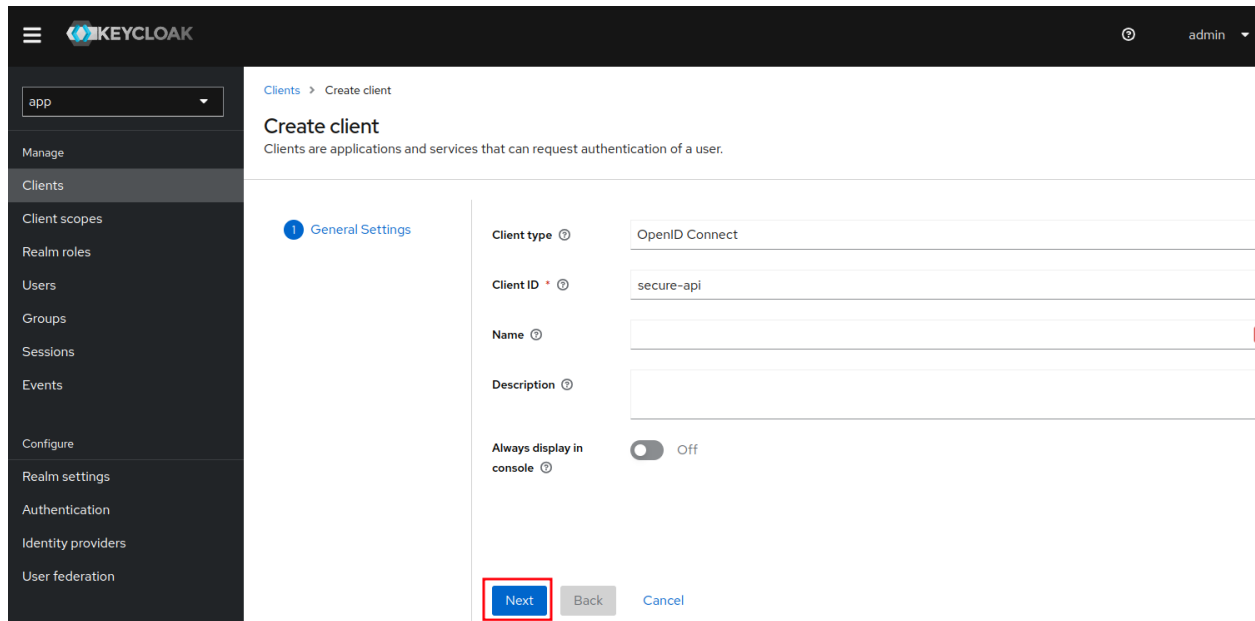
3) After the realm be created with success, click on the Tokens tab and change the Access Token Lifespan to 1 day.



4) Click on the Clients menu and after that, click the Create client button. PS: Make sure all steps are executed inside **app** Realm.

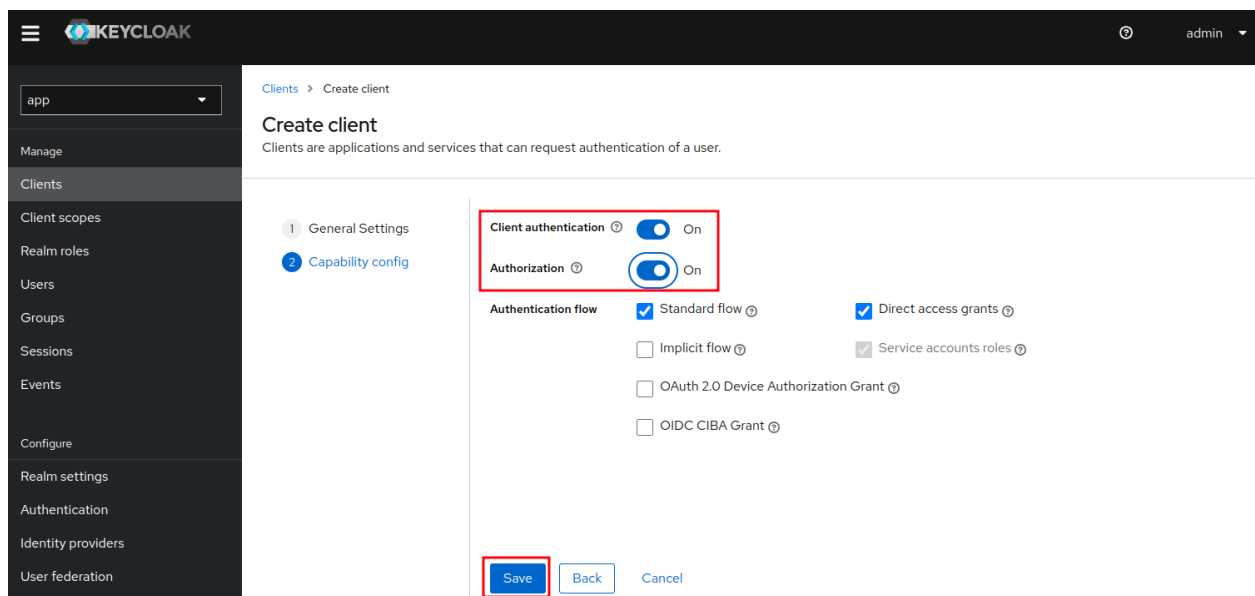


5) Fill the name with the client as **secure-api** and click the next button.



The screenshot shows the 'Create client' page in Keycloak. The left sidebar contains a menu with options: Manage, Clients, Client scopes, Realm roles, Users, Groups, Sessions, Events, Configure, Realm settings, Authentication, Identity providers, and User federation. The 'Clients' menu item is selected. The main content area is titled 'Create client' and includes a sub-header 'Clients are applications and services that can request authentication of a user.' Below this, the 'General Settings' tab is active. The form fields are: 'Client type' (OpenID Connect), 'Client ID' (secure-api), 'Name' (empty), and 'Description' (empty). There is a toggle for 'Always display in console' which is currently 'Off'. At the bottom, there are three buttons: 'Next' (highlighted with a red box), 'Back', and 'Cancel'.

6) Enable Client authentication and Authorization. Click Save button.



The screenshot shows the 'Create client' page in Keycloak, specifically the 'Capability config' tab. The 'General Settings' tab is still selected in the left sidebar. The main content area shows the 'Capability config' section. The 'Client authentication' and 'Authorization' toggles are both turned 'On' and are highlighted with a red box. Below these, the 'Authentication flow' section has a checked box for 'Standard flow' and unchecked boxes for 'Implicit flow', 'OAuth 2.0 Device Authorization Grant', and 'OIDC CIBA Grant'. The 'Direct access grants' section has a checked box for 'Direct access grants' and a checked box for 'Service accounts roles'. At the bottom, there are three buttons: 'Save' (highlighted with a red box), 'Back', and 'Cancel'.

7) Go to the Clients menu again and click on the client you just created. Change the options to match the configuration below and click the Save button.

Client ID [?] secure-api

Name [?]

Description [?]

Always display in console [?] ☐ Off

Access settings

Root URL [?]

Home URL [?]

Valid redirect URIs [?] http://localhost:8081/* [?]

[Add valid redirect URIs](#)

Valid post logout redirect URIs [?] + [?]

[Add valid post logout redirect URIs](#)

[Save](#) [Revert](#)

Jump to section

- General Settings
- Access settings
- Capability config
- Login settings
- Logout settings

8) Click on the Realm Roles menu, click Create role button.

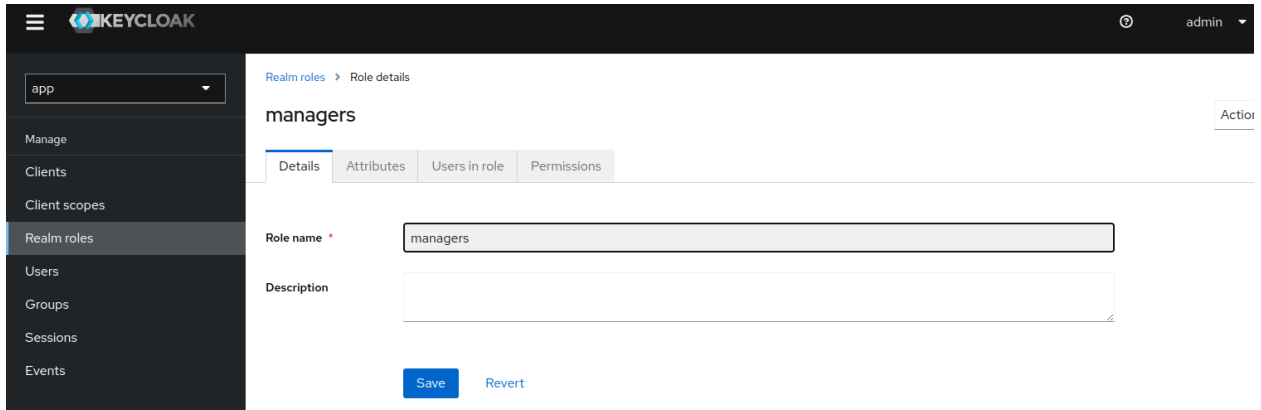
Realm roles

Realm roles are the roles that you define for use in the current realm. [Learn more](#)

[→](#) [Create role](#) 1 - 5

| Role name | Composite | Description |
|--|-----------|------------------------------|
| default-roles-app [?] | True | `\${role_default-roles}` |
| managers | False | — |
| offline_access | False | `\${role_offline-access}` |
| operators | False | — |
| uma_authorization | False | `\${role_uma_authorization}` |

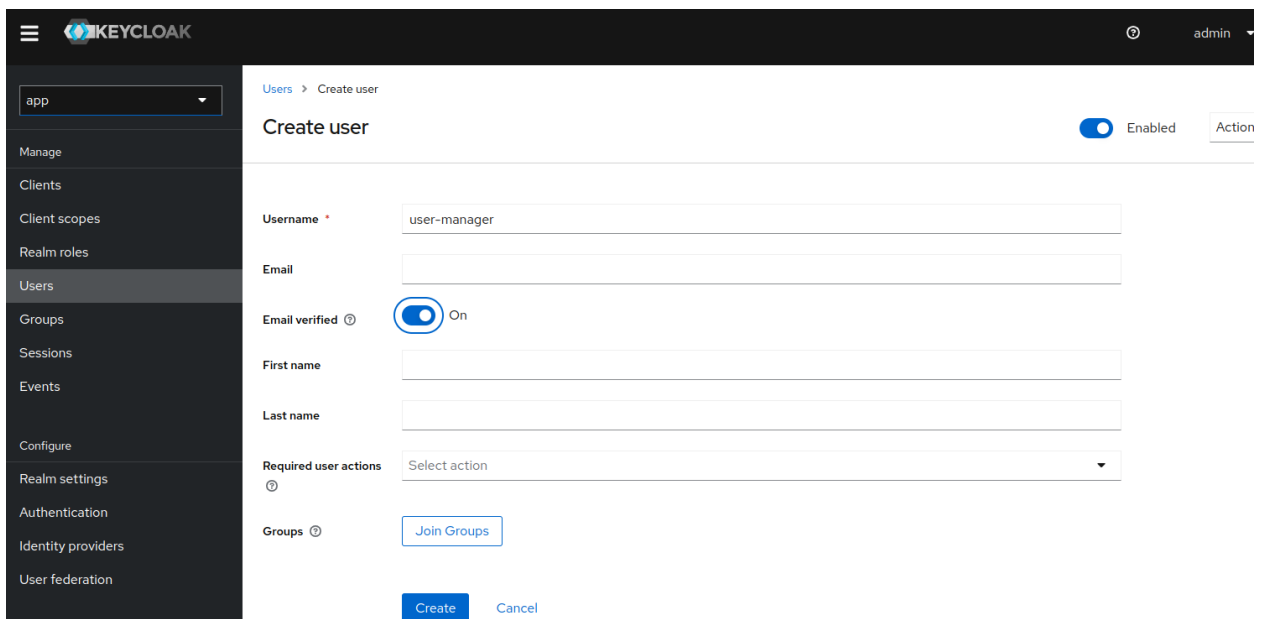
9) Fill the Role name input with **managers** and click the Save button.



The screenshot shows the Keycloak administration interface. On the left is a dark sidebar with a menu containing: Manage, Clients, Client scopes, Realm roles (highlighted), Users, Groups, Sessions, and Events. The main content area is titled 'managers' under the 'Role details' section. It has four tabs: Details (active), Attributes, Users in role, and Permissions. The 'Role name' field contains 'managers'. The 'Description' field is empty. At the bottom are 'Save' and 'Revert' buttons. The top right shows the user 'admin'.

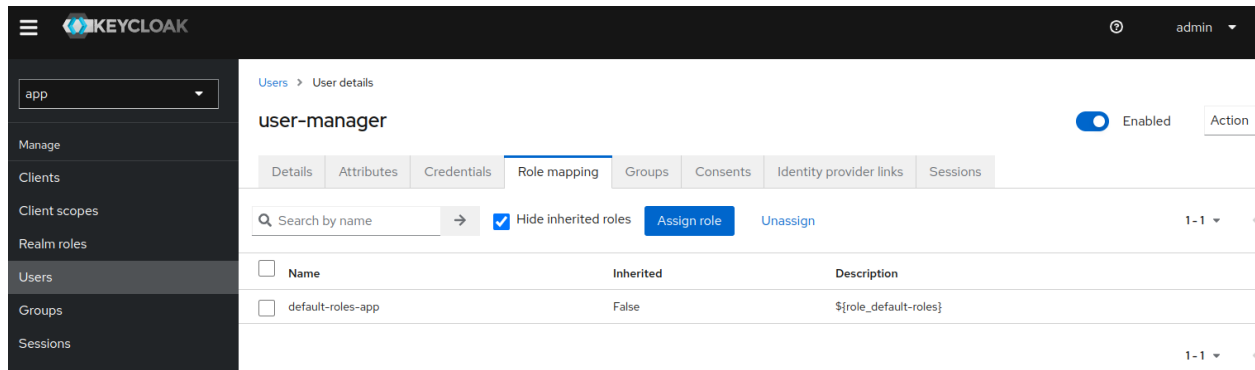
10) Repeat the last two steps to create another role called **operators**.

11) Go to the Users menu, click on Add user button, fill in the Username field **user-manager** and click the Create button.

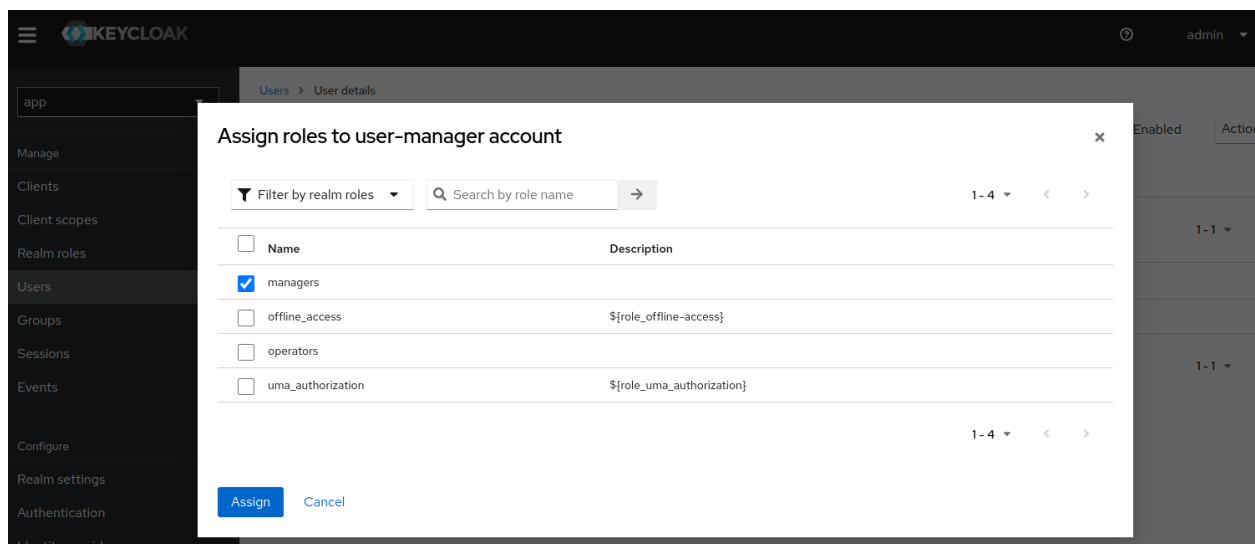


The screenshot shows the 'Create user' page in Keycloak. The sidebar menu has 'Users' highlighted. The main content area is titled 'Create user' and has an 'Enabled' toggle switch turned on. The 'Username' field contains 'user-manager'. The 'Email' field is empty. The 'Email verified' toggle switch is turned on. The 'First name' and 'Last name' fields are empty. The 'Required user actions' dropdown is set to 'Select action'. There is a 'Join Groups' button. At the bottom are 'Create' and 'Cancel' buttons. The top right shows the user 'admin'.

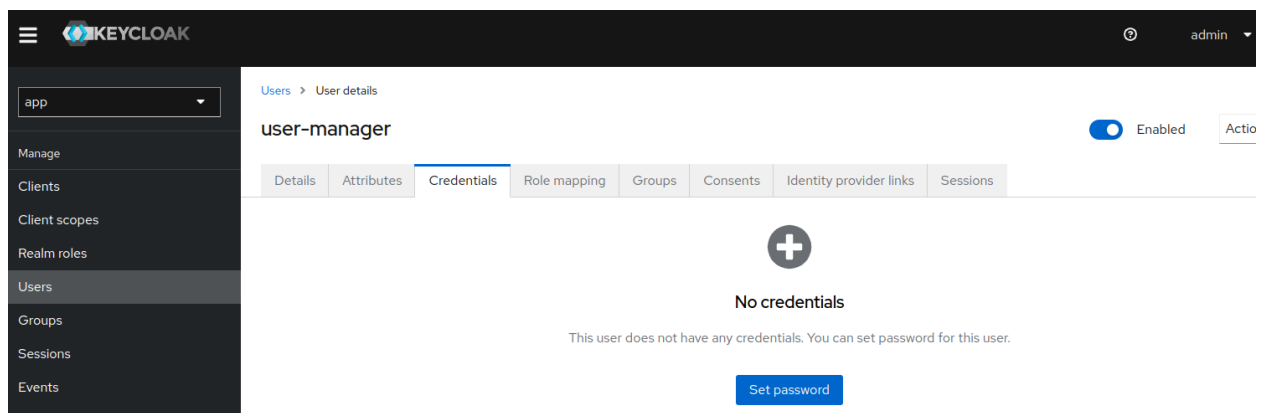
12) Go to the Role Mappings tab and click Assign role button.



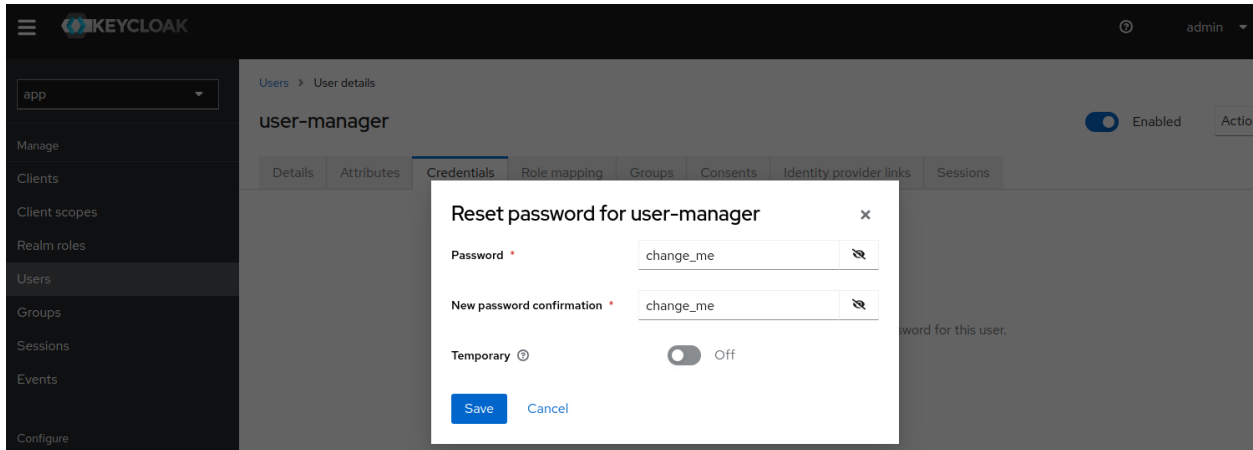
13) Select **managers** and click Assign button again.



14) Go on the Credentials tab and click Set password button.



15) Create a password and click Save button.



13. Repeat from step #10 to create another new user with username **user-operator**, and make sure to use the role **operators** inside the Role Mappings.